Finansdepartementet
103 33 Stockholm

Remiss av SOU 2023:61 – En säker och tillgänglig statlig e-legitimation

Fi2023/02704

1 Sammanfattning

Skatteverket välkomnar initiativ som leder till digital identifiering av hög tillförlitlighet och tillgänglighet då det skapar förutsättningar för myndigheten att bedriva en högkvalitativ och tillgänglig verksamhet samt möjliggör minskat utrymme för identitetsrelaterad brottslighet.

Skatteverkets bedömning är att det föreligger ett tydligt behov av att utreda frågorna på ett mer sammanhållet sätt för att uppnå utredningens avsedda effekter. Ett helhetsperspektiv gällande digital identitet är en förutsättning för att kunna uppnå en sammanhållen identitetsförvaltning. En ny e-legitimation är bara en pusselbit i detta. I det här remissvaret lämnas därför synpunkter av avgörande och principiell vikt angående de delar av förslaget där Skatteverket anser att det krävs ytterligare förtydliganden och överväganden för att bestämmelserna ska kunna tillämpas på det sätt som lagstiftaren avser.

Skatteverkets synpunkter tar främst sikte på att e-legitimationen måste vara användarvänlig. Eftersom det finns flera alternativ på marknaden måste det finnas en robusthet och användarkvalitet i statens e-legitimation. Till exempel bör e-legitimationen kunna användas genom mobiltelefon. Risken med att inte ta ett helhetsgrepp tidigt i processen innebär att det kommer saknas incitament för personer att över huvud taget införskaffa sig ännu en e-legitimation.

Utredningen föreslår en ansökningsavgift för att finansiera delar av det arbete som fordras för att utföra grundidentifieringen. Skatteverket upplever att en separat ansökningsprocess i kombination med en hög avgift utgör en risk för att många inte kommer se nyttan med att skaffa sig den nya e-legitimationen.

Utredningen förordar Polismyndigheten framför Skatteverket i fråga om att genomföra grundidentifieringen. Skatteverket instämmer i denna bedömning.

Skatteverket anser att det är av betydande vikt att den fortsatta beredningen av statlig e-legitimation utforskar möjligheterna för upptagning och lagring av biometri i syfte att kontrollera och verifiera identitet både för privata och offentliga aktörer.

Vad gäller ekonomiska konsekvenser så ansluter sig Skatteverket till utredningens bedömning.

Postadress: 205 30 MALMÖ **Telefon**: 0771-567 567
skatteverket@skatteverket.se, www.skatteverket.se

2 Skatteverkets synpunkter

2.1 Definitioner av vissa centrala begrepp och termer (3)

Skatteverket anser att det vore lämpligt att definiera begreppet identitet ytterligare. En mer tydlig definition vore fördelaktig för att tydliggöra vad det är som kontrolleras av den identitetskontrollerande myndigheten. Då det endast är ett fåtal identitetsattribut som lagras kopplat till identitetsbeteckningen samordningsnummer tolkar Skatteverket – till skillnad från utredningen - inte denna identitetsbeteckning som en synonym till eIDAS definition av termen ”Personidentifieringsuppgift” som de menar ska kunna användas för att fastställa identiteten på en fysisk eller juridisk person.

Om enbart de identitetsattribut som utredningen inkluderar i sin definition av identitet (namn, födelsetid och som huvudregel medborgarskap) används är graden av återidentifierbarhet låg. Det vill säga att med dessa attribut kan det finnas många olika identiteter i registret med olika identitetsbeteckningar. Med ett styrkt samordningsnummer har Skatteverket kontrollerat den fysiska personens biometri mot en identitetshandling men de attribut som utgör själva identiteten är tämligen sparsamma.

2.2 Internationell utblick (5)

Skatteverket önskar – med anledning av synpunkterna i remissvaret – en mer omfattande beskrivning av e-legitimation i andra medlemsstater där det dras mer djupgående slutsatser kring varför ett land har valt en viss lösning och hur väl denna lösning anses fungera.

2.3 Utformning av den statliga e-legitimationen (7.2)

Utredningen föreslår en statlig e-legitimation endast på högsta nivå. Det medför att en statlig e-legitimation inte kommer kunna användas via mobiltelefon. E-legitimation på lägre nivåer som kan användas via mobiltelefon skulle öppna upp för att fler kan använda den statliga e-legitimationen och att fler skulle vilja uppdatera till den högre nivån genom att gå från en lägre nivå till en högre. Användarvänligheten riskerar dessutom gå förlorad när digitala lösningar inte erbjuds. Risken med att inte ta höjd för detta är att komplikationer skjuts över på användarna istället för att det omhändertas av det offentliga. Att endast ha e-legitimation på högsta nivå riskerar att stänga ute en stor del av befolkningen från en säkrare statlig e-legitimation.

Med hänvisning till ovan är frågan hur de beträffande målgrupperna äldre och personer med funktionsnedsättning skulle vara mer hjälpta av en statlig e-legitimation. Skatteverket menar att det saknas incitament för målgruppen att välja sig av den statliga e-legitimationen i stället för befintliga lösningar såsom Bank-Id och Freja.

Till skillnad från utredningens förslag i avsnitt 7.2.2 om att den statliga e-legitimationen ska tillhandahållas på ett kontaktlöst kort är Skatteverkets bild att ett fysiskt ID-kort borde kopplas till e-legitimationskortet och det borde vara på det nationella ID-kortet redan från start. Separat ansökan och därmed separat kostnad skulle i sådana fall enbart nyttjas i de fall individen inte har möjlighet att få dessa ID-handlingar utfärdade.

Det bör även tilläggas att e-legitimation på ett fysiskt separat kort förmodligen medför att folk i allmänhet inte kommer ha sitt eventuellt införskaffade kort med sig till vardags, vilket medför låg användningsgrad även bland innehavare av e-legitimationen.

Skatteverket anser sammantaget att bristen på användarvänligenhet kommer medföra att få personer införskaffar samt använder sig av den föreslagna statliga e-legitimationen.

2.4 Grundidentifiering (7.5)

Såväl i betänkandets sammanfattning som i avsnitt 6.3 anges att med grundidentifiering avses i detta betänkande ett förfarande som leder fram till att en identitetshandling utfärdas. Denna ska innefatta en process i vilken det ingår personlig inställelse för sökanden vid såväl ansökan som vid utlämnandet av identitetshandlingen. Skatteverket uppfattar detta som att det krävs personlig inställelse vid två tillfällen.

I avsnitt 7.5 anger utredningen att den ansluter sig till DiGG:s förslag om utgivningsprocess. Där anges det att en fördel med förslaget är att utgivningsprocessen innebär att ansökan, grundidentifiering, utlämnade och, i förekommande fall, aktivering av e-legitimationen kan ske vid ett och samma tillfälle (SOU 2023:61, s. 153).

Skatteverket önskar ett förtydligande kring hur detta ska förstås. Förutsatt att säkerheten inte påverkas förordar Skatteverket en så smidig process som möjligt för kund.

2.5 Ansvar för grundidentifierande och utfärdande (7.6)

I avsnitt 7.6.2. har utredningen övertygande och noggrant redovisat vad som krävs ur olika aspekter för att ansvara för grundidentifiering och identitetskontroll. Att det läggs stor vikt vid att motverka bedrägeribrottsligheten gör sig fortsatt gällande och talar inte för Skatteverket som ansvarig för att utföra grundidentifieringen. Polismyndigheten hanterar redan idag lagring av biometriska uppgifter och har dessutom stor erfarenhet av identifiering.

Skatteverket delar utredningens bedömning om att Polismyndigheten är lämpad att utföra uppdraget.

2.6 Giltighetstid och återkallelse (7.7)

Skatteverket har i sig inget att invända mot utredningens utgångspunkt i avsnitt 7.7.2 att giltighetstid för den statliga e-legitimationen bör beakta säkerhetsriskerna med en alltför lång giltighetstid. Dock bör även användarperspektivet och administrationsbördan vid en för kort giltighetstid framhållas. Utredningen föreslår högst fem år som giltighetstid.

Argumentet att utseendet förändras mycket vid en längre giltighetstid är inte tillräckligt om fingeravtryck ska lämnas och om det framöver kommer finnas möjligheter till kontroll av biometriska uppgifter. Det är mindre användarvänligt för privatpersoner om dessa ska behöva förnya olika typer av id-handlingar (såsom pass, nationellt id-kort och körkort) med förhållandevis täta intervall. Utredningen utvecklar inte frågan om administrationsbördan.

För att ta hänsyn till användarperspektivet bör e-legitimationen i varje fall som huvudregel gälla sju år. Som exempel kan nämnas att det tyska nationella identitetskortet är försett med en e-legitimation på tillitnivån hög i kortets chip och giltighetstiden är 10 år för användare som är 24 år och äldre.

Gällande avsnitt 7.7.2 om återkallelse och spärr av den statliga e-legitimationen har Skatteverket synpunkter på den rättsliga formuleringen. I 12 § första stycket tredje punkten i den föreslagna lagen om elektronisk identifiering anges att återkallelse och spärr ska ske bl.a. om det är nödvändigt av säkerhetsskäl för att någon annan än den som medlet är utställt till kan misstänkas obehörigt förfoga över det, eller om innehavaren av medlet på annat sätt förlorat kontrollen över det.

Lagtexten innehåller genom detta en precisering som begränsar vilka säkerhetsskäl som kan ligga till grund för återkallelse och spärr, dvs. situationer där någon annan än den medlet är utställt till råder över det eller innehavaren på annat sätt förlorat det. I SOU 2019:14 föreslogs att en e-legitimation skulle kunna återkallas av säkerhetsskäl, utan att det preciserades vilka specifika säkerhetsskäl som skulle vara aktuella i lagtexten. En av situationerna som togs upp i motiven var den när en säkerhetsbrist upptäcks som möjliggör bedräglig användning (SOU 2019:14 s. 347). En sådan återkallelse sker på grund av en befarad framtida bedräglig användning, vilket faller utanför lagtextens ordalydelse om misstänkt obehörigt förfogande.

Enligt Skatteverket bör även andra säkerhetsskäl än de uppräknade kunna vara aktuella för återkallelse. Situationen där någon använder sin egen e-legitimation som ett led i ett brottsligt förfarande (t.ex. bedrägerier) faller i nuläget utanför lagtextens ordalydelse, eftersom själva förfogandet kan vara behörigt. Lydelsen tillåter inte heller t.ex. återkallelse om personen är föremål för internationella sanktioner, vilket i många fall utgör grund för återkallelse av t.ex. BankID.

Enligt Skatteverket bör lagtexten inte avgränsa säkerhetsskälen som kan vara aktuella, varför bestämmelsen kan få följande lydelse:

12 § Ett statligt medel för elektronisk identifiering ska återkallas och spärras om

[...]

3. det är nödvändigt av säkerhetsskäl,

Om lagtexten får den föreslagna utformningen, bör även säkerhetsskäl införas som en grund för att avslå en ansökan om statligt medel för elektronisk identifiering. En sådan reglering kan införas i 10 § och ha följande lydelse:

10 § En ansökan ska avslås om förutsättningarna i 5 och 6 §§ inte är uppfyllda. Detsamma gäller om det som anges i 8 § eller som föreskrivits i enlighet med 11 § andra stycket 1 inte har iakttagits, och sökanden inte har följt en uppmaning att avhjälpa bristen. En ansökan ska vidare avslås om förutsättningar för återkallelse enligt 12 § första stycket 3 föreligger.

2.7 Användningen av den statliga e-legitimationen (7.8)

Skatteverket har i dagsläget inte rätt att lagra, eller använda lagrade, biometriska uppgifter. I den fortsatta beredningen bör det beaktas att en identitetskontrollerande myndighet inte fullt ut kan kontrollera att den unika personen kopplas till rätt identitet, via korrekt identitetsbeteckning, då det saknas lagstöd för att säkerställa att identiteterna är unika genom att jämföra biometriska egenskaper med lagrade värden. Skatteverket anser att det här är aspekter som bör utredas i samband med en statlig e-legitimation.

Detta förfarande tillsammans med de få identitetsattribut som lagras vid tilldelning av samordningsnummer medför att det finns utmaningar med att säkerställa att personen är unik i Sverige vid grundregistrering av en person och etablering av en identitet vid flytt till Sverige (då det inte finns några biometriska kännetecken lagrade att jämföra emot). Det som kan kontrolleras är att det är sannolikt att de identitetshandlingar som presenteras överensstämmer med den fysiska personen som presenterar dem för att styrka samordningsnummer.

Rättsliga möjligheter till, och kontroll mot, lagrade biometriska egenskaper skulle motverka risken för missbruk. Ett större antal identitetsattribut vid tilldelning av samordningsnummer skulle vidare kunna öka förståelsen av vem man interagerar med vid användning av en e-legitimation genom uppslag i registret.

Den identitetskontrollerande myndigheten kommer enligt utredningens förslag att kunna använda biometriska kännetecken för att identifiera en fysisk person och kontrollera att dess biometriska egenskaper är unika i utgivarens databas, och säkerställa att det är en unik person. De kan dock inte fullt ut kontrollera att den unika personen kopplas till rätt identitet då Skatteverket saknar lagstöd för att säkerställa att identiteterna är unika genom att jämföra biometriska egenskaper med lagrade värden.

Skatteverket anser att en helhetsbedömning är väsentlig för att e-legitimationen ska kunna användas i samhället på ett tryggt sätt.

2.8 Finansiering av den statliga e-legitimationen (7.9)

Utredningen föreslår att kostnaderna för utfärdandet av den statliga e-legitimationen och grundidentifieringen ska i huvudsak finansieras via anslag. En ansökningsavgift föreslås finansiera delar av det arbete som fordras för att utföra grundidentifieringen. Den som ansöker om en statlig e-legitimation föreslås betala en avgift som motsvarar den som erläggs vid ansökan om pass eller nationellt identitetskort, enligt förordningsförslaget 400 kr. Avgiften för att få en statlig e-legitimation och avgifter för användning av e-legitimationen kommer att bidra med viss, men inte full, kostnadstäckning.

Beträffande förslaget om avgift är Skatteverkets bild att detta utgör en tröskel för att få användare att skaffa sig en statlig e-legitimation. Den statliga e-legitimation kommer att verka i konkurrens med t.ex. Bank-ID som tillhandahålls bankkunderna kostnadsfritt, eller i varje fall utan särskild avgift vid utfärdandet. Det kan antas att den som redan har Bank-ID och är nöjd med den tjänsten inte med någon större sannolikhet kommer att anse att det statliga alternativet erbjuder något mervärde. I varje fall så länge inte fler tjänster som uppfattas som nödvändiga och attraktiva förutsätter innehav av en statlig e-legitimation.

Det lyfts i avsnitt 9.9 i utredningen att kravet på personlig inställelse i anskaffningsprocessen kan medföra kostnader, särskilt för vissa målgrupper. Ett giltigt svenskt pass eller giltigt svenskt nationellt identitetskort är en förutsättning för två av de tre föreslagna sätten att aktivera e-legitimationen. Om den enskilde inte har någon av dessa handlingar, utan måste ansöka om sådana, bör det inte förbises att också det kan ses som en kostnad ur ett användarperspektiv.

En separat ansökningsprocess för enbart e-legitimation i kombination med hög avgift gör alltså att det finns anledning att misstänka att de flesta inte ens kommer se nyttan med att skaffa sig den nya statliga e-legitimationen. Även om enskilda kan få ekonomiskt bistånd riskerar det att bli dubbla trösklar då man först måste söka ekonomiskt bistånd för att därefter kontakta myndigheterna för att kunna få statlig e-legitimation.

Utredningen argumenterar för en ansökningsavgift, inte främst för att den bidrar till kostnadstäckningen vid grundidentifieringen, utan för att den är avsedd att inskärpa att den statliga e-legitimationen är en värdehandling. Detta bör dock ställas i relation mot att det uppgivna syftet med en statlig e-legitimation är att stärka samhällets säkerhet och robusthet, motverka bedrägerier som begås med hjälp av e-legitimationer och underlätta för så många som möjligt att kunna få tillgång till en säker e-legitimation. Förvaltningspolitiskt har det i olika sammanhang kommit fram en ambition att Sverige ska profilera sig som ledande inom digital förvaltning. Den ambitionen torde förutsätta att samtliga individer garanteras möjlighet att använda tillförlitliga elektroniska identitetshandlingar.

Sammantaget medför ansökningsavgiften och ansökningsprocessen att införskaffandet av en ny statlig e-legitimation inte blir så omfattande som utredningen önskar, utan begränsas till personer som för närvarande har svårt att få en id-handling men har ett samordningsnummer och styrkt identitet. Det bör således övervägas i den fortsatta beredningen om staten ska se en statlig e-legitimation som en nationell angelägenhet/kollektiv nyttighet och tillskjuta ytterligare anslagsmedel som täcker hela kostnaden för grundidentifieringen för att förstärka intresset för användningen.

2.9 Konkurrensrättsliga frågor (7.10)

Skatteverket avser inte gå in på närmare bedömningar och synpunkter gällande konkurrensrättsliga frågor. Skatteverket vill dock, som i avsnittet ovan, konstatera att den största privata aktören utfärdar Bank-ID gratis.

Den argumentation som förs i 7.10.1 om att syftet med den föreslagna statliga e-legitimationen inte är att konkurrera utan att komplettera till privata alternativ kan diskuteras. Avsikten får anses vara att tillhandahålla lösningar som är säkrare än befintliga aktörers, både på individ- och samhällsnivå, och dessutom tillgängliga för fler. Förhållandet att staten i rådande säkerhetsläge tar ansvar för att minska sårbarheten och öka tillgängligheten, dvs. ökar krisberedskapen, torde vara ett allmänt intresse som kan beaktas inom ramen för konkurrensrätten.

2.10 Behandling av personuppgifter (7.11)

Betänkandet föreslår att den utfärdande myndigheten ska ha rätt att föra en databas över statliga e-legitimationer. Begreppet ”databas” återfinns därför bl.a. i 16–18 §§ i den föreslagna lagen om elektronisk identifiering. Enligt författningskommentaren är utformningen i denna del hämtad från lagen (2015:899) om identitetskort för folkbokförda i Sverige. I betänkandet Framtidens dataskydd vid Skatteverket, Tullverket och Kronofogden (SOU 2023:100) föreslås att databasregleringen för dessa myndigheter ska upphävas. Där framhålls bl.a. att databas är ett juridiskt begrepp och inte avser en tekniskt avgränsad databas.

Med tanke på den snabba tekniska utvecklingen inom det digitala området kan det vara värt att även i detta sammanhang överväga om begreppet databas ska användas över huvud taget. Detsamma gäller för begreppet ”direktåtkomst” som nämns i avsnitt 7.11.9. I SOU 2023:100 föreslår man mot bakgrund av den tekniska utvecklingen och innehållet i EU:s dataskyddsförordning att direktåtkomst bör likställas med övriga former av elektroniskt utlämnande.

2.11 Sekretess (7.12)

De uppgifter som kommer att behandlas automatiserat inom föreslagen databas hos den utfärdande myndigheten kommer enligt förslaget att vara sekretessreglerade genom 22 kap. 1 § offentlighet- och sekretesslagen (2009:400) (OSL). Av denna bestämmelse följer att sekretess föreligger för uppgift om en enskilds personliga förhållanden, om det av särskild anledning kan antas att den enskilda eller någon denna närstående lider men om uppgifterna röjs.

Även helt rättsenliga åtgärder kan innebära att skada eller men uppkommer för en enskild. I förarbetsuttalanden till den tidigare sekretesslagen – till vilket det hänvisas i förarbetena till OSL – angavs som exempel att någon har blivit föremål för framgångsrika indrivningsåtgärder eller att någon har blivit satt i fängelse, intagen för sluten psykiatrisk vård eller ställd under övervakning (prop. 1979/80:2 Del A s. 83 samt prop. 2008/09:150 s. 350). Detta följer även av rättspraxis.

Att den utfärdande myndigheten tillhandahåller en brottsbekämpande myndighet uppgifter i enlighet med de sekundära ändamålen i 20 § tredje stycket 1 och 2 förslag till lag om elektronisk identifiering kan enligt Skatteverket innebära ett sådant röjande att det får anses föreligga särskild skäl att anta att den enskilda lider men om uppgifterna röjs. Det finns därför enligt Skatteverkets bedömning behov av en sekretessbrytande bestämmelse för att möjliggöra tillhandahållandet av uppgifter från den utfärdande myndigheten till en brottsbekämpande myndighet. Det kan här noteras att den bestämmelse som följer av 6 kap. 5 § OSL inte är sekretessbrytande.

Skatteverket delar bedömningen att det inte finns något behov av en sekretessbrytande bestämmelse för de uppgifter som inhämtas från Skatteverket för sådana primära ändamål som följer av 20 § första och andra stycket förslag till lag om elektronisk identifiering.

Skatteverket delar även bedömningen att det inte finns något behov av en sekretessbrytande bestämmelse inom den brottsbekämpande verksamheten i de fall uppgifter har gjorts gemensamt tillgänglig och den mottagande myndigheten behöver uppgifterna i sin brottsbekämpande verksamhet.

2.12 Krav om att godta identifiering med vissa e-legitimationer (7.13)

Såsom utredningen föreslagit tillstyrker Skatteverket att ska det vara ett lagkrav att samtliga offentliga aktörer erkänner identifiering med den föreslagna e-legitimationen. Den bör fungera i alla offentliga e-tjänster som kräver elektronisk identifiering om den uppfattas som relevant samt vara så inkluderande som förutsätts i utredningen. För ett ökat förtroende bör även privata aktörer ansluta sig, så att kunden inte behöver ha flera olika e-legitimationer. För att få en ökad vilja från privata marknaden kan staten t.ex. välja att låta aktörer koppla upp sig kostnadsfritt.

Definitionen av vilka som är offentliga aktörer är omfattande. Hur kravet ska fungera i praktiken och om ikraftträdandetiden för bestämmelsen behöver anpassas till aktörernas olika förutsättningar är ganska summariskt behandlat i 8 kap. i utredningen och bör möjligen utvecklas.

Såsom föreslås i 7.13.6 är det lämpligt att det ges en viss möjlighet att göra undantag från kraven. Särskilt viktig är bedömningen och förslagen att det med hänsyn till rikets säkerhet kan behöva tas hänsyn till vissa myndigheters verksamhet och bemyndiganden att meddela föreskrifter om undantag.

2.13 Ikraftträdande- och övergångsbestämmelser (8)

Lagkravet att samtliga offentliga aktörer ska erkänna identifiering med den föreslagna e-legitimationen ska fungera i praktiken kommer med en del anpassningar. En annan ikraftträdandetid för den bestämmelsen kan behöva övervägas närmare.

3 Konsekvenser för Skatteverket

Skatteverket har inga invändningar mot de kostnader som redovisas i SOU 2023:61.

Detta remissvar har beslutats av generaldirektören Katrin Westling Palm och föredragits av juristen Tommy Nieminen. Vid den slutliga handläggningen har också följande deltagit: överdirektören Fredrik Holmberg, avdelningschef Peter Sävje och enhetschef Karolin Wallström.

Katrin Westling Palm